DETAILED ACTION

1. This office action is response to applicant's amendment filed on December 16, 2009 for the application No: 10/555408.

2. Applicant's arguments have been considered but have been found not persuasive.

Applicant's Arguments

3. Applicant's arguments:

I. Applicant argues that the cited prior art does not disclose "input device is a mouse and wherein the data interception unit is configured to passively collect mouse data generated in response to the user", stating:

a. Matchett does not disclose a mouse

b. The data generated is not mouse data

c. Data is not passively collected since user is aware of mouse and user does not use the mouse no data is collected.

d. The data collected is physiological and not behavioral

II. Applicant argues that the cited prior art does not disclose "dynamically monitoring and passively collecting behavioral biometric information from a mouse", stating (other than was stated in I) is that Akiyama does not teach passively collecting mouse data

III. Transparently collecting data

Examiner's response to applicant's arguments

4. Applicant's arguments/ amendments with respect to pending claims 1-5, 7-12, 14, and 19-26 filed September 8, 2009, have been fully considered but have been found not persuasive.

In response to applicant's arguments:

I.

a. Applicant admits Matchett discloses a thumbscanning or hand geometry mouse with out further need to go into more detail applicant please do not accuse applicant of being contradictory, just say the argument is not persuasive contradicts himself by stating a mouse is not a mouse. The type of mouse is irrelevant.

b. The data is collected using the mouse and concerning certain properties of the mouse hence it is "mouse data"

c. User is aware of mouse in the instant application and user does not need to use the mouse in the instant application as well. If the mouse is not used no data will be collected. Furthermore Matchett discloses data is collected passively in column 13 lines 14-28.

d. Matchett discloses in column 12 lines 11-30, among data collected and of interest is hand pressure characteristics and typing pattern recognition which are behavioral characteristics and Matchett also states that devices be concealed. For example the key pattern recognition is installed in computer keypad. It would be obvious to conceal/modify the hand pressure characteristics obtaining device with a mouse. Matchett in figures 8A and 8B shows other types of data which can be collected by modifying a mouse.

II. Examiner stated in the previous office action that Akiyama collects data based on mouse movement. Matchett discloses the rest of the limitation as discussed in I.

III. Passively collecting data is transparent to the user, see Matchett column 12 lines 62-63 user does not need to perform any actions that he would not normally perform. By collecting data passively and not requiring user to perform any additional actions implies that the collection of data is transparent.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-2, 4-5, 7-12, 19-26 are rejected under 35 U.S.C. 103(a) as being unpatentable by Brown et al. (U S Patent Number 5,557,686) in view of Matchett (US Patent # 5,229,764) and further in view of Akiyama et al. (US Patent Number 5,768,387).

As per claims 1, 25 and 26, Brown discloses: a behavioral biometrics based user verification system for use with an input device, said system comprising a data interception unit for receiving inputs from a user, - Brown, column 2 lines 15-19, collecting samples containing typing characteristics of an authorized user based on key press times and key release times is a behavioral biometrics based system which intercepts data from a user,

a behavior analysis unit operatively coupled to said data interception unit - Brown, column 2 lines 20-22, vectors constructed for purifying the samples are behavioral analysis units since they contain behavioral data,

and a behavior comparison unit operatively coupled to said interception unit, wherein said system translates behavioral biometrics information into representative data.

- Brown, column2 lines 28-29, the neural network trained to output whether an input is from an authorized user is representative data of biometric information,

stores and compares different results, and outputs a user identity result - Brown, column 2 lines 30-32 and 38-38, the user typing the previously determined keystroke sequence into the neural network then having the neural network determine whether the user is authorized, is storing and comparing the different results and outputting the user identity result.

But fails to disclose expressly the input device is a mouse and wherein the data interception unit is configured to passively collect mouse data generated in response to the user;

However, Matchett discloses that the input device is a mouse and wherein the data interception unit is configured to passively collect mouse data generated in response to the user; - Matchett, figure 11 and column 13, lines 12-28, data input unit is a mouse which is a device used for collecting data passively

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the passively collecting mouse movement data method of Matchett with the behavioral biometric based system of Brown because having a continuous authentication method makes theft more difficult and less likely since it continuously checks up on registered user - Matchett, column 2, lines 59-63, column 3 lines 2-3.

But Brown in view of Matchett does not explicitly disclose that the passively collected data is mouse movement data

However Akiyama discloses: wherein said data interception unit is configured to identify data based on mouse movement - Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Brown with the teaching of Akiyama in order to provide input devices as a keyboard or a mouse, or both as pointed out in Akiyama. - Akiyama, column 11 lines 39-41, input devices can be keyboard and mouse

As for claim 25, mouse data collected passively without user knowledge, is mouse data collection initiated, collected and terminated passively if any of the steps are not passive the collection of the mouse data is not passive.

As for claim 26, mouse data collected passively without user knowledge, is mouse data collection initiated, collected and terminated passively if any of the steps are not passive the collection of the mouse data is not passive. Passively collecting data is transparent to the user.

As per claim 2, Brown in view of Matchett and further in view of Akiyama discloses: The user verification system of claim 1, wherein said system is suitably configured for real-time monitoring - Brown, column 13 lines 52-55, system notifying a system operator that user has not passed keystroke is real-time monitoring

As per claim 5, Brown in view of Matchett and further in view of Akiyama discloses: the limitations of claim 4, wherein said data interception unit is further configured to characterize movement based on at least one of average speed, average traveled distance, and direction of movement. - Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement.

As per claim 7, Brown in view of Matchett and further in view of Akiyama discloses: the limitations of claim 1, wherein said data interception unit is further configured to identify action from a mouse as one of drag and drop, point and click, mouse movement, and silence, such that in use, said system receives data from a mouse - Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement.

As per claim 8, Brown in view of Matchett and further in view of Akiyama discloses: the limitations of claim 1 but fails to disclose expressly the limitation in claim 7, wherein said data interception unit is further configured to characterize movement based on at least one of average speed, average traveled distance, and direction of movement. - Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement.

As per claims 20, Brown in view of Matchett and further in view of Akiyama discloses the system of claim 1, wherein the behavior comparison unit is configured to produce the user identity result based on mouse movement speed compared to traveled distance, average speed per direction of movement, a distribution of movement directions, average speed with respect to action type, a distribution of actions, a distribution of traveled distance, and a distribution of movement elapsed time. - Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement, It would be obvious for one skilled in the art at the time of the invention to use any combination calculations related to the mouse movement and a factor.

As per claim 24, Brown in view of Matchett and further in view of Akiyama discloses the system of claim 1, wherein the behavior analysis unit is configured to establish a user signature based on a plurality of sessions in an enrollment mode. –Brown, column2 , lines 12-25, multiple user samples are used in authentication process.

As per claim 9, Brown discloses: A method of characterizing a user comprising the steps of moving motion based input device, dynamically monitoring and passively collecting behavioral biometric information from input device, - Brown, column 2 lines 15-19, a keyboard is a motion-based input device which is used to collect data,

a processing said passively collected behavioral biometric information, - Brown column 2 lines 20-22, vectors constructed for purifying the samples are behavioral analysis units since

they contain behavioral data and column2 lines 28-29, the neural network trained to output whether an input is from an authorized user is representative data of biometric information,

developing a signature for a user based on the processed information - Brown column 2 lines 30-32 and 38-38, the user typing the previously determined keystroke sequence into the neural network then having the neural network determine whether the user is authorized is a model of users signature.

But fails to disclose expressly that the input device is a mouse.

However, Matchett discloses that the input device is a mouse - Matchett, figure 11 and column 13, lines 12-28, data input unit is a mouse which is a device used for collecting data passively

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the passively collecting mouse movement data method of Matchett with the behavioral biometric based system of Brown because having a continuous authentication method makes theft more difficult and less likely since it continuously checks up on registered user - Matchett, column 2, lines 59-63, column 3 lines 2-3.

But Brown in view of Matchett does not explicitly disclose that the passively collected data is mouse movement data

However Akiyama discloses: wherein said data interception unit is configured to identify data based on mouse movement - Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Brown with the teaching of Akiyama in order to provide input devices as a keyboard or a mouse, or both as pointed out in Akiyama. - Akiyama, column 11 lines 39-41, input devices can be keyboard and mouse

As per claim 4 and 22, Brown in view of Matchett and further in view of Akiyama discloses: the limitations of claim 1 and 9 respectively, wherein said data interception unit is configured to identify data based on mouse movement and is not associated with a mouse click - Matchett, figure 11 and column 13, lines 12-28, data input unit is a mouse and passively collects data

wherein said data interception unit is configured to identify data based on mouse movement between first and second locations, wherein movement between the first and second locations is not associated with a mouse click - Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement.

As per claim 10, Brown in view of Matchett and further in view of Akiyama discloses: The method of claim 9, further comprising comparing said signature with a signature of an authorized user - Brown, column 2 lines 30-32 and 38-38, the user typing the previously determined keystroke sequence into the neural network then having the neural network determine whether the user is authorized is a model of users signature.

As per claim 11, Brown in view of Matchett and further in view of Akiyama discloses: The method of claim 10, further comprising filtering said data after processing and before developing the signature to reduce noise - Brown, column 4 lines 30-35, purifying users input files is filtering the processed data before modeling and reduces noise.

As per claim 12, Brown in view of Matchett and further in view of Akiyama discloses: The method of any one of claims 11, further comprising collecting and processing and developing the signature in real-time - Brown, column 14 lines 7-18, continuously updating the users profile with new samples is a method which collects, processes and models data in real-time, modeling the data is the user signature.

As per claims 14, Brown in view of Matchett discloses: the limitations of claim 9, wherein said collecting data further comprises characterizing movement based on at least one of average speed, average traveled distance, and direction of movement -Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement.

As per claim 19, Brown in view of Matchett and further in view of Akiyama the system of claim 1, wherein the behavior comparison unit is configured to store user identities for a plurality of potential users, and the user identity result identifies the user from among the plurality of potential users. – Brown, column2, lines 16 and 17, plurality of users are authorized for system, i.e. authentication information is stored for multiple users of the system

As per claim 21, Brown in view of Matchett and further in view of Akiyama discloses the method of claim 9, wherein the signature for the user is developed based on movement speed compared to traveled distance, average speed per direction of movement, distribution of movement directions, average speed with respect to action type, a distribution of actions, a distribution of traveled distance, and a distribution of movement elapsed time. - Akiyama, figure 8 and column 11 lines 42-46, the input device is a mouse and the tracks of the mouse movement are detected, tracks are the path of the mouse and hence are the direction of movement, It would be obvious for one skilled in the art at the time of the invention to use any combination calculations related to the mouse movement and a factor.

As per claim 23, Brown in view of Matchett and further in view of Akiyama discloses the method of claim 9, wherein the behavioral biometric information from the mouse is obtained in a background process. - Matchett, figure 11 and column 13, lines 12-28, data input unit is a mouse which is a device used for collecting data passively, passively collecting data without user knowledge is performed as a background process else user will know about the process.

7. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brown in view of Matchett in further view of Akiyama and Boebert et al. (US Patent Number 5,596,718).

As per claim 3, Brown in view of Matchett and further in view of Akiyama discloses: the limitations of claim 2

But fails to disclose expressly: further comprising secure communication protocols operatively couple to said data interception unit.

Boebert discloses: further comprising secure communication protocols operatively couple to said data interception unit; - Boebert, column 3 lines 26-29, an inserted trusted path between input/output devices and work station is a secure communication protocol between the system and data interception.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the secure communication between input device and system of Boebert with the behavioral biometric based system of Brown because it would deter malicious hard ware or software from emulating and listening to the communication path between the user and system - Boebert, column 1 lines 30-35.

Conclusion

8. **THIS ACTION IS MADE FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

9. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SIMON KANAAN/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432